FF

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-288973
(43)Date of publication of application : 28.11.1990

(51)Int.CI. G06F 15/30
G06F 15/00
G06K 17/00
G07F 7/12

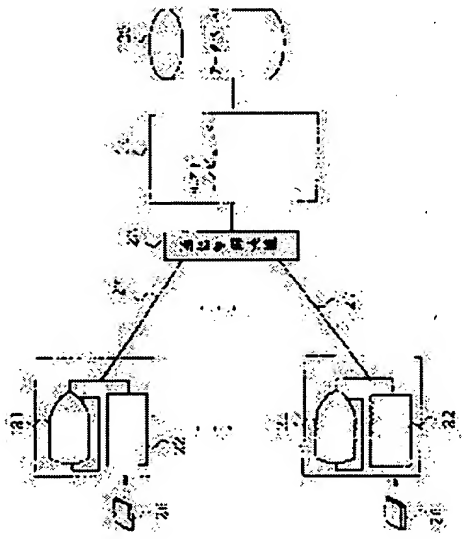
(21)Application number : 01-051554
(22)Date of filing : 03.03.1989

(71)Applicant : RICOH CO LTD
(72)Inventor : SHOJI HIROYUKI
FURUTA TERUYUKI

(30)Priority
Priority number : 64 2312 Priority date : 09.01.1989 Priority country : JP

(54) SYSTEM FOR PROTECTING PRESUMPTION OF PASSWORD

(57)Abstract:
PURPOSE: To heighten the security of a system by displaying camouflage information and taste information set at every digit corresponding to an access key, and confirming a password by collating information selected and inputted from a display content by a customer with the taste information registered on a card.
CONSTITUTION: The output picture data of the camouflage information(Camouflage Information:CI) including the information of credit balance and transaction specification, etc., and individual taste information(Individual Taste Information:ITI) used in the definition of the password is registered on a data base 25. Also, a host computer 24 stores a program for the confirming processing of the password. And a owner confirming processing is performed by displaying the output picture data accumulated in the data base 25 on terminal equipment 21 according to the information read from the card 26 inserted by the customer and collating data selected and inputted from the terminal equipment 21 by the customer according to the above display with owner identification information set in advance, and furthermore, an automatic transaction is performed. In such a way, the security of the system can be heightened than ever.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2−288973

⑤1Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)11月28日
G 06 F 15/30	340	6798−5B	
15/00	330 F	7361−5B	
G 06 K 17/00	V	6711−5B	
G 07 F 7/12		8208−3E	

G 07 F 7/08　C

審査請求　未請求　請求項の数 2　（全17頁）

⑤4発明の名称　暗証番号の推測防護方式

⑳特　願　平1−51554

㉒出　願　平1(1989)3月3日

優先権主張　㉜平1(1989)1月9日㉝日本(JP)㉛特願　平1−2312

⑦2発明者　庄司　浩之　東京都大田区中馬込1丁目3番6号　株式会社リコー内

⑦2発明者　古田　輝幸　東京都大田区中馬込1丁目3番6号　株式会社リコー内

⑦1出願人　株式会社リコー　東京都大田区中馬込1丁目3番6号

⑦4代理人　弁理士　磯村　雅俊

明細書

1.発明の名称

暗証番号の推測防護方式

2.特許請求の範囲

(1)本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、上記カードには、個人的な嗜好や特徴を含む情報を基にして各桁の番号を定義した暗証番号と、該暗証番号の各桁毎に設定された偽装情報へのアクセスキーとを含むデータを登録し、上記システムには、該アクセスキーに対応する該偽装情報を含むデータを格納して、顧客が挿入したカードにより該暗証番号の各桁の番号を照合して本人であることを確認する場合には、該アクセスキーに対応して各桁毎に設定した該偽装情報、および該嗜好情報を表示して、顧客が表示内容から選択・入力した情報と該カードに登録された該嗜好情報とを照合して、該暗証番号を確認することを特徴とする暗証番号の推測防護方式。

(2)本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、該システムには、ID番号、本人確認を行う際の照合コードの生成に用いるアルゴリズム、該照合コードの構成、および該アルゴリズムの演算要素として用いる乱数の桁数を含むデータを登録し、顧客が上記カードを用いて該システムへアクセスする場合には、該システムは該カードからID番号を読み取り、該乱数桁数に従って乱数を発生して表示するとともに、登録されたアルゴリズムに該乱数を代入して照合コードを生成し、該照合コードと、顧客が入力したコードとを比較照合して、本人確認を行うことを特徴とする暗証番号の推測防護方式。

3.発明の詳細な説明

〔技術分野〕

本発明は、暗証番号を利用して本人確認を行う銀行システム等における暗証番号の推測防護方式に関し、特に、システムのセキュリティを高める

ことが可能な暗証番号の推測防護方式に関する。

〔従来技術〕

従来、銀行システム等では、各種サービスを行う際に顧客本人であることを確認するため、予め顧客毎に暗証番号を決め、その暗証番号を利用して本人確認を行っていた。また、暗証番号には数値4桁程度の組み合わせの固定コードが採用され、顧客は記憶し易い番号(例えば生年月日等)を設定していた。

この暗証番号は主に人間の記憶よって保護されているため、大幅に桁数を増やすことは難しい。このため、顧客が設定した暗証番号を、第3者が推測し、被害届が出されるまで繰返し不正使用されることがあった。

さらに、桁数の多いコードを採用したり、推測され難い数字を登録した場合でも、そのコードを記憶するためのメモ等が必要となり、メモを紛失すると本人でもアクセスできなくなる。

また、コンピュータサービスシステムでは、コンピュータ端末を使ってアクセスする場合等、不

正な利用者が思いついたコードによるアクセスを試行してパスワードを探り当てる恐れがあった。

なお、コンピュータ・システムのセキュリティについては、例えば“デー・ダブリュー・デービス，ダブリュー・エル・プライス著，セキュリティ フォー コンピュータ・ネットワーク，ジョン・ウィリィ アンド サンズ，１９８４，(D.W. Davies, W.L.Price: Security for computer networks, John Wiley& Sons, １９８４)”において論じられている。

〔発明が解決しようとする課題〕

上記従来技術では、暗証番号の桁数を増加したり、固定コード以外の照合コードを登録することによって、システムのセキュリティを高めることが難しかった。

本発明の目的は、このような問題点を改善し、システムのセキュリティを高めることが可能な暗証番号の推測防護方式を提供することにある。

〔課題を解決するための手段〕

上記目的を達成するため、本発明の暗証番号の

推測防護方式は、本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、上記カードには、個人的な嗜好や特徴を含む情報を基にして各桁の番号を定義した暗証番号、その暗証番号の各桁毎に設定された偽装情報へのアクセスキー等を登録し、上記システムの出力画面データファイルには、そのアクセスキーに対応する偽装情報を格納して、顧客が挿入したカードにより暗証番号の各桁の番号を照合して本人であることを確認する際、画面制御部の制御により、アクセスキーに対応して各桁毎に設定した偽装情報、および嗜好情報を表示して、顧客がその表示内容から選択・入力した情報とカードに登録された嗜好情報とを照合処理部で照合して、その暗証番号を確認することに特徴がある。

また、本発明の暗証番号の推測防護方式は、本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、そのシステムのアクセスコー

ド情報ファイルには、上記カードのＩＤ番号、本人確認を行う際の照合コードの生成に用いるアルゴリズム、その照合コードの構成、およびそのアルゴリズムの演算要素として用いる乱数の桁数を含むデータを登録し、顧客がカードを用いてシステムへアクセスする場合には、システムのアクセスコード情報読取部はそのカードからＩＤ番号を読み取り、乱数発生処理部は登録された桁数に従って乱数を発生して、その乱数を顧客に対して表示するとともに、アクセスキーコード作成処理部は登録されたアルゴリズムにその乱数を代入して照合コードを生成し、入力コード照合処理部によってその照合コードと、顧客が入力したコードとを比較照合して、本人確認を行うことに特徴がある。

〔作用〕

本発明においては、個人的な嗜好や特徴を含む情報を基にして暗証番号の各桁を定義し、本人確認を行う際は、その暗証番号の各桁毎に設定された偽装情報を表示して、選択・入力させるため、

顧客に負担を与えることなく、暗証番号の桁数を増加することができる。

また、本発明においては、本人確認に用いる照合コードとして、固定された数字列を用いず、その照合コードを生成するためのアルゴリズムを登録し、そのアルゴリズムの演算要素として、システムが発生させた乱数、あるいは年月日、時刻、曜日、任意の変数等を用いるため、本人以外の不正な使用者が照合コードを類推することは難しい。

これらの方法を採用することにより、システムのセキュリティをより高めることが可能である。

〔実施例〕

以下、本発明の一実施例を図面により説明する。

まず、本発明の第１の実施例について述べる。

第２図は、本発明の第１の実施例における自動取引システムの構成図である。

本実施例の自動取引システムは、銀行の各店舗毎に端末装置２１およびカード読取装置２２を備え、銀行の顧客は本人確認情報(暗証番号)を記憶したカード２６を利用して自動的に入出金取引を

行う。また、これらの装置２１，２２は、通信回線２７および通信制御装置２３を介してホストコンピュータ２４に接続される。さらに、ホストコンピュータ２４にはデータベース２５が接続される。

この端末装置２１は、顧客が本人識別情報（暗証番号）を入力する際に用い、また、必要に応じてホストコンピュータ２４からのメッセージを出力する。

また、カード読取装置２２は、顧客により挿入されたカード２６の内容を読み取ってホストコンピュータ２４に渡す。

また、データベース２５は、預金残高、取引種別等の情報や、暗証番号を定義する際に用いた個人的な嗜好情報(Individual Taste Information：ＩＴＩ)を含む偽装情報(Camouflage Information：ＣＩ)の出力画面データを登録する。

また、ホストコンピュータ２４は、暗証番号の確認処理を行う際のプログラムを格納する。

これにより、顧客が挿入したカード２６から読

み取った情報に従って、データベース２５に蓄積された出力画面データを端末装置２１に表示し、その表示に従って顧客が端末装置２１から選択・入力したデータと、予め設定した本人識別情報とを照合して、本人確認処理を行い、さらに自動取引を行う。

第３図は、本発明の第１の実施例における登録データ例図、第４図は本発明の第１の実施例におけるカード作成方法の説明図である。

本実施例では、顧客が自動取引を行う際に使用するカードの登録データは、個人的な嗜好情報(以下ＩＴＩと記す)等を基に作成する。つまり、第３者が推測し難い情報（本人の好きな色、身体特徴、趣味)を基に登録データを作成する。

さらに、カード作成時に、ＩＴＩ情報とともに、偽装情報(以下ＣＩと記す)も登録する。

例えば第３図のように、暗証番号の１桁目～４桁目のそれぞれに対応するＩＴＩ情報およびＣＩ情報を登録データとする。この場合、ＩＴＩ情報は本人を識別するための真の情報であり、ＣＩ情

報は第３者による暗証番号の推測を防止するための偽装情報である。

また、第４図のように、カード４１には暗証番号を直接登録せず、ＩＴＩ情報番号およびシステム内に記憶したＣＩ情報へのアクセスキーを登録する。これは、ＣＩ情報をカード内に登録すると、第３者によって解読される恐れがあるためである。なお、ＣＩ情報はシステム内に記憶する。

従って、カード４１を作成する手順としては、銀行側(サービス提供者側)は予め全顧客に対応するＩＴＩ情報とＣＩ情報を作成し、ＣＩ情報へのアクセスキー番号を設定する。次に、顧客は自分のＩＴＩ情報を決定する。次に、銀行側では顧客が指定したＩＴＩ情報の値で自動取引用のカード４１を作成して、顧客に提供する。これにより、顧客はＩＴＩ情報を従来の暗証番号のように記憶する必要はない。すなわち、自動取引時の本人確認では、ＩＴＩ情報およびＣＩ情報を含む画面が表示されるため、本人の嗜好や特徴にあった項目を指示することにより暗証番号を入力できる。

第５図は、本発明の第１の実施例における自動取引システムの機能構成図である。

本実施例の自動取引システムは、カード読取部５２、出力画面データファイル５３、画面データ読込み処理部５４、画面制御部５５、入力データ処理部５６、照合処理部５７、およびカード返却部５８を備える。

このカード読取部５２は、顧客が挿入したカード５１の内容を読み込み、画面データ読込み処理部５４は、カード５１内に登録されたＣＩ情報へのアクセスキーをもとに、データベース２５に格納された出力画面データファイル５３から該当画面データを読み込む処理を行う。

また、画面制御部５５は、顧客の入力に応じて表示する画面データを制御する。

また、入力データ処理部５６は、表示画面の項目から顧客が選択した真の番号の入力データを処理する。なお、この入力データ(真の番号)は照合処理に使用される。

また、照合処理部５７は、カード内に記憶されたＩＴＩ情報と、入力データ処理部５６により入力された真の番号とを照合する。

また、カード返却部５８は、処理終了後、顧客から挿入されたカード５１を返却する。

第１図は、本発明の第１の実施例における自動取引システムの本人確認処理を示すフローチャート、第６図は本発明の第１の実施例における表示画面例図である。

このような構成により、本実施例の自動取引システムにおいて本人確認を行う場合には、第１図のように、顧客から挿入されたカードを読み込み(１０１)、そのカードに対応するＣＩ情報へのアクセスキーおよびＩＴＩ情報を記憶する(１０２)。

次に、ＩＴＩインデクスを１とし(１０３)、ＣＩ情報のアクセスキーによって、その顧客用の画面データを画面データファイル５３から読み出す(１０４)。

その画面データを端末装置２１にガイダンスとともに表示する(１０５)。例えば第６図①のように好きな色を問う画面が表示される。この場合、

顧客が選択すべき真の番号は３である。これにより、顧客は表示された項目の番号から真の番号を選択して入力する。

次に、顧客が入力した番号と、カード内のＩＴＩ情報とが一致する場合には(１０６)、ＩＴＩインデクスの値を１アップし(１０７)、次の画面データを表示する。さらに、全ＩＴＩ情報の照合が終了するまで(１０８)、暗証番号(４桁)の各桁に対応する画面が第６図②～④のように表示され、顧客の入力とカード内のＩＴＩ情報との照合が行われる。

こうして全ての項目(４種類)について照合が完了し、登録した全てのＩＴＩ情報が一致すると、顧客本人であることを確認し(１０９)、自動取引を行う(１１０)。

また、顧客が入力した番号と、カード内のＩＴＩ情報とが一致しない場合には、照合エラー用の画面データを読み出して表示する(１１１)。

これらの処理が終了すると、顧客にカードを返却し(１１２)、処理を終了する。

なお、第１図におけるｎはＩＴＩ情報数であり、暗証番号が４桁の場合にはｎ＝４である。

次に、本発明の第２の実施例について述べる。

本実施例の自動取引システムは、第１の実施例(第２図)と同様に、端末装置、カード読取装置、通信回線、ホストコンピュータ、およびデータベースを備え、顧客は本人確認情報を記憶したカードを利用して自動的に入出金取引を行う。

特に本実施例では、本人確認情報として定数を登録せず、照合コードを生成するためのアルゴリズムを登録し、さらに演算要素として定数および乱数を使用する。また、演算子として、＋，－，×，÷，(　)，mod(ａ，ｂ)等が使用できる。但し、÷は商の整数部、(　)は演算順序を規定するための括弧、mod(ａ，ｂ)はｂをａで割った剰余である。さらに、アクセスキーコードは、顧客の希望によって分割することが可能であり、各部分ごとにアルゴリズムを設定できる。また、演算結果が照合コードの桁数を超える場合は溢れた上位桁を捨て、また演算結果が負数の場合には絶対値を充てる。

また、データベースには、預金残高、取引種別等の情報や、本人確認情報を定義する際に用いるアクセスコード情報(ＡＣＩ)を登録したアクセスコード情報ファイルを格納する。なお、アクセスコード情報としては、ＩＤ番号、照合コード（アクセスキーコード）を生成するためのアルゴリズム、キーコード構成、そのアルゴリズムの演算要素として用いる乱数の桁数等を登録する。

また、ホストコンピュータは、照合コードの確認処理を行う際のプログラムを格納する。

このような構成により、顧客が挿入したカードから読み取ったＩＤコードによりデータベースに蓄積されたアクセスコード情報を読み出し、乱数を発生して端末装置に表示し、その表示に従って顧客が端末装置から入力したコードと、予め登録したアルゴリズムにその乱数を代入して生成したコードとを照合して、本人確認処理を行い、さらに自動取引等のサービス提供を行う。

第７図は、本発明の第２の実施例における自動取引システムの機能構成図である。

第７図において、７１はカード読取装置、７２はカード読取部、７３はアクセスコード情報（ＡＣＩ）ファイル、７４はディスプレイ制御部、７５はアクセスコード情報読取部、７６は乱数発生処理部、７７はアクセスキーコード(ＡＫＣ)作成処理部、７８は入力コード照合処理部、７９はキーボード読取部、８０はサービス提供機能、８１は端末装置のディスプレイ、８２は端末装置のキーボード(ＫＢ)である。

このカード読取部７２は、カード読取装置７１が顧客のカードから読み取ったＩＤコードを受け取り、アクセスコード情報読取部７５に渡す。

また、アクセスコード情報読取部７５は、カードのＩＤコードにより、アクセス情報ファイル７３から該当するアクセスコード情報を読み出し、乱数発生処理部７６およびアクセスキーコード作成処理部７７に渡す。

また、乱数発生処理部７６は、アクセスコード情報読取部７５から渡されたアクセスコード情報(乱数桁数)によって乱数を発生し、ディスプレイ

制御部７４およびアクセスキーコード作成処理部７７に渡す。

また、アクセスキーコード作成処理部７７は、アクセスコード情報読取部７５より得たアクセスコード情報(コード構成、生成アルゴリズム)と、乱数発生処理部７６より得た乱数とから、照合コードを生成し、入力コード照合処理部７８に渡す。

また、入力コード照合処理部７８は、キーボード読取部７９を介して顧客から得た入力コードと、アクセスキーコード作成処理部７７より得た生成コードとを比較照合し、その結果がＯＫならば、サービス提供機能８０へサービス許可の指示を出し、結果がＮＧならば、その通知をディスプレイ制御部７４に渡す。

また、ディスプレイ制御部７４は、端末装置のディスプレイ８１を制御して、アクセスコード入力の案内、および乱数発生処理部７６が発生した乱数を表示し、また、コード照合結果をメッセージとともに表示する。

次に、本実施例における本人確認処理を具体的な例を挙げて述べる。

第８図は、本発明の第２の実施例におけるアクセスキーコードの構成例図、第９図は本発明の第２の実施例におけるアクセスコード情報例図、第１０図は本発明の第２の実施例における自動取引システムの本人確認処理を示すフローチャートである。

本実施例では、契約時、顧客は“乱数の桁数”、“アクセスキーコードの構成”、および“照合コードを生成するためのアルゴリズム”を決定する。

例えば、乱数の桁数を４とし、アクセスキーコードの構成を第８図のようにC_1(２桁)，C_2，C_3の４桁として、アルゴリズムを“$C_1=50-RN_1$，$C_2=RN_1+RN_2$，$C_3=RN_4+1$”とする。なお、RN_1，RN_2，RN_4はシステムが発生させる乱数の１，２，４桁目を示し、３桁目の乱数は表示されるのみで、照合コードの生成には用いられない。

また、システム側は、顧客の申告をＩＤ番号と対応させてアクセスコード情報ファイル７３に記

憶する。

例えば、第９図のように、ＩＤ番号“１２３４５６”、乱数桁数“４”、キーコード要素数“３”、要素C_1の桁数“２”、要素C_1へのポインタ、要素C_2の桁数“１”、要素C_2へのポインタ、要素C_3の桁数“１”、要素C_3へのポインタ、およびアルゴリズム記述“$C_1=50-RN_1$，$C_2=RN_1+RN_2$，$C_3=RN_4+1$”をアクセスコード情報ファイル７３に記憶する。

こうして契約手続きが終了した後、顧客はカードを用いてサービスの提供を要求することができる。

すなわち、第１０図のように、顧客がカードをカード読取装置７１に挿入して読み取らせるか、あるいはＩＤ番号をキーボード８２から入力すると(１００１)、システム側では、そのＩＤ番号に対応するアクセスキーコード情報をアクセスコード情報ファイル７３から読み出して(１００２)、メモリに記憶する。

さらに、このアクセスキーコード情報により、

乱数桁数が４桁であることを知り、４桁の乱数を発生させて、メッセージとともにディスプレイ８１に表示する(１００３)。例えば、乱数を“$RN_1=5$，$RN_2=9$，$RN_3=4$，$RN_4=1$”とする。

この表示により、顧客は予め登録したアルゴリズムを想い出し、表示された乱数をそれに代入してアクセスキーコードを作成し、キー入力する。

この場合、$C_1=50-RN_1=50-5=45$，$C_2=RN_1+RN_2=5+9=14$，$C_3=RN_4+1=1+1=2$となり、“４５４２”をキー入力する。なお、C_2は計算結果が予め決められた桁数を超えるため、下位の１桁を採る。また、表示された乱数の中、第３桁($RN_3=4$)は使用されないが、これは本人以外の利用者を惑わせるためである。

一方、システム側では、読み取ったアクセスキーコード情報から、アクセスキーコードを作成するアルゴリズム（要素数、各要素の桁数、各要素を算出する式）を知り、顧客に対して表示した乱数を当てはめて、“４５４２”を生成する(１００４)。

こうしてアクセスキーコードの入力が完了すると(１００５)、顧客が入力したアクセスキーコードとシステム側で生成したコードとを比較照合する(１００６)。

その結果、一致すれば(１００７)、システムのサービス提供を許可し、一致しなければ（１００７）、ディスプレイ８１にエラーメッセージを出力する(１００８)。

なお、本実施例では、４桁のアクセスキーコードを発生するアルゴリズムとして、乱数の第３桁を使用しない場合を示したが、この他にも種々の方法が考えられる。

例えば、乱数４桁で、アクセスキーコード構成を４要素各１桁(C_1，C_2，C_3，C_4)とし、アルゴリズムを$C_1=9$，$C_2=RN_4$，$C_3=RN_3$，$C_4=RN_2$とする。これにより、上位の１桁のみが固定的に“９”となり、その他は乱数によって変化するため、乱数“２０６８”を発生させた場合には、アクセスキーコードは“９８６０”となる。

また、例えば乱数９桁で、アクセスキーコード構成を３要素（C_1は２桁、C_2，C_3は１桁)とし、アルゴリズムを$C_1=100-RN_1\times RN_2$，$C_2=RN_1+RN_2$，$C_3=RN_9$とする。これにより、９桁の乱数を発生しても、実際に用いるのは３桁であるため、容易に記憶でき、乱数“４６３８３１２０６”を発生させた場合には、アクセスキーコードは“８４０６”となる。

このように、提示する乱数は、１桁毎に分離して用いたり、全体を１個の数として使用したり、全く使用しない桁を設けたり、あるいは、同じ桁の数字を繰返して使用することができるため、多様なアルゴリズムを設定することが可能である。

また、パスワード中に本実施例の数列を組み込むことにより、コンピュータ端末からのアクセス時に、デタラメなコードを何度も試して正しいコードを探り当てる方法に対処することができる。

次に、本発明の第３の実施例について述べる。

本実施例の自動取引システムは、第１の実施例

(第２図)と同様に、端末装置、カード読取装置、通信回線、ホストコンピュータ、およびデータベースを備え、顧客は本人確認情報を記憶したカードを利用して自動的に入出金取引を行う。

また、本人確認情報として定数を登録せず、照合コードを生成するためのアルゴリズムを登録する。特に、演算要素として、年(Ｙ)、月(Ｍ)、日(Ｄ)、時刻(Ｈ)、曜日(Ｗ)、定数、および顧客が代入する変数値(V_S(設定)、V_R(参照))等であり、複数使用する場合はV_{Si}のようにサフィックスを付ける)を使用する。さらに、演算子として、＋，－，×，÷，(　)，mod(ａ，ｂ)等を使用する。

但し、÷は商の整数部、(　)は演算順序を規定するための括弧、mod(ａ，ｂ)はｂをａで割った剰余である。さらに、年(Ｙ)、月(Ｍ)、日(Ｄ)、時刻(Ｈ)および曜日(Ｗ)は、顧客がシステムにアクセスした時点の値を適用する。

また、V_Sは顧客が任意の数値を代入できる部分であり、その値はアクセスキーコードの別の部分を生成するために参照する。その参照値としての表現形がV_Rである。例えば、アクセスキーコードを２桁の数(C_1，C_2)とし、$C_1=V_S$，$C_2=9-V_R$とした場合を述べる。顧客が第１桁に任意の数字“３”を入力し、C_2のV_Rに“３”を代入すると、$C_2=9-3=6$となり、正しい入力コードは３６である。このように、V_Sは$C_K=V_S$の形で定義する。これらの演算要素により、より多様なアルゴリズムを設定できる。

また、データベースには、預金残高、取引種別等の情報や、本人確認情報を定義する際に用いるアクセスコード情報(ＡＣＩ)を登録したアクセスコード情報ファイルを格納する。なお、アクセスコード情報としては、ＩＤ番号、照合コード(アクセスキーコード)を生成するためのアルゴリズム、キーコード構成を登録する。

また、ホストコンピュータは、照合コードの確認処理を行う際のプログラムを格納する。

第１１図は、本発明の第３の実施例における自動取引システムの機能構成図である。

第１１図において、７１はカード読取装置、

７２はカード読取部、７３はアクセスコード情報(ＡＣＩ)ファイル、７４はディスプレイ制御部、７５はアクセスコード情報読取部、７７はアクセスキーコード(ＡＫＣ)作成処理部、７８は入力コード照合処理部、７９はキーボード読取部、８０はサービス提供機能、８１は端末装置のディスプレイ、８２は端末装置のキーボード(ＫＢ)である。

このカード読取部７２は、カード読取装置７１が顧客のカードから読み取ったＩＤコードを受け取り、アクセスコード情報読取部７５に渡す。

また、アクセスコード情報読取部７５は、カードのＩＤコードにより、アクセス情報ファイル７３から該当するアクセスコード情報を読み出し、アクセスキーコード作成処理部７７に渡す。

また、アクセスキーコード作成処理部７７は、アクセスコード情報読取部７５より得たアクセスコード情報(コード構成、生成アルゴリズム)から、生成コードを生成し、入力コード照合処理部７８に渡す。　また、入力コード照合処理部７８は、キーボード読取部７９を介して顧客から得た入力コードと、アクセスキーコード作成処理部７７より得た生成コードとを比較照合し、その結果をディスプレイ制御部７４に渡す。

また、ディスプレイ制御部７４は、端末装置のディスプレイ８１を制御して、アクセスコード入力の案内、およびコード照合結果をメッセージとともに表示する。

次に、本実施例における本人確認処理を具体的な例を挙げて述べる。

第１２図は、本発明の第３の実施例におけるアクセスコード情報例図、第１３図は本発明の第３の実施例における自動取引システムのアクセス時の処理を示すフローチャートである。

本実施例では、顧客との契約時にアクセスコードの構成および算出アルゴリズムを決定する。

例えば、アクセスコードは４桁として、４個の構成要素に分割し、各構成要素は１桁とする。つまり、C_1，C_2，C_3，C_4を構成要素とする。また、算出アルゴリズムは、$C_1=V_S$、$C_2=1$、$C_3=V_R+H$、$C_4=5+\mathrm{mod}(3，D)$とする。

この内容を、顧客のＩＤコードと対応させてアクセスコード情報ファイル７３に登録する。すなわち、第１２図のように、ＩＤコード“１２３４５６”、キーコードの要素数“４”、要素１の桁数“１”、要素１へのポインタ、要素２の桁数“１”、要素２へのポインタ、要素３の桁数“１”、要素３へのポインタ、要素４の桁数“１”、要素４へのポインタ、およびアルゴリズム記述“$C_1=V_S$、$C_2=1$、$C_3=V_R+H$、$C_4=5+\mathrm{mod}(3, D)$”を登録する。

こうして契約を行い、システムへアクセスする場合には、第１３図のように、顧客は磁気カードをカード読取部７２に読み取らせるか、あるいはＩＤコードをキーボード８２から入力する（１３０１）。

これにより、アクセス情報読取部７５は、ＩＤコードに対応するアクセスキーコード情報をアクセスコード情報ファイル７３より読み出し、メモリへ記憶する（１３０２）。

次に、ディスプレイ制御部７４の指示により、

アクセスコード入力を促すメッセージをディスプレイに表示する（１３０３）。

この表示に従い、顧客は契約時に登録したアルゴリズムを想い出してキーコードを入力する。例えば、$C_1=V_S$として任意の数字“７”をキーインし、C_2には固定の値“１”を入力する。また、$C_3=V_R+H$には、$V_S=7$、および現在の時刻“１２時”からH＝１２を代入し、７＋１２＝１９を得るが、桁数が溢れているため、下１桁をとって$C_3=V_R+H=9$を入力する。さらに、本日が“１３日”であることから、$C_4=5+\mathrm{mod}(3, D)=5+\mathrm{mod}(3, 13)=5+1=6$を入力する。

こうしてアクセスコードが入力されると（１３０４）、アクセスキーコード作成処理部７７は、アクセスコード情報からアクセスキーコード構成と生成アルゴリズムを知り、顧客が入力したV_S、システムで管理している日付、時刻等を代入して、コードを生成する（１３０５）。

次に、入力コード照合処理部７８は、アクセスキーコード作成処理部７７で生成したコードと、

顧客が入力したアクセスキーコードとを比較照合し（１３０６）、一致すれば（１３０７）、サービス提供を許可する。また、一致しなければ、エラー処理を行う（１３０８）。

〔発明の効果〕

本発明によれば、自分の暗証番号を直接記憶する必要がないため、４桁前後の暗証番号に限定されることはなく、また、本人の嗜好や特徴等の情報を基にして定義するため、第３者が暗証番号を推測することは難しい。これにより、暗証番号の桁数を増加させることができる。

また、本発明によれば、アルゴリズムは無意味な数字よりも記憶し易く、逆に他人が推測することは難しい。さらに、そのアルゴリズムの演算要素としてシステムが発生させた乱数、あるいは年月日、時刻、曜日、任意の変数等を利用するため、アルゴリズムが推測できなければ、仮に、デタラメな入力でキーコードが偶然に一致することあっても、カードを連続して不正使用することはできない。

従って、システムのセキュリティをより高めることが可能である。

4.図面の簡単な説明

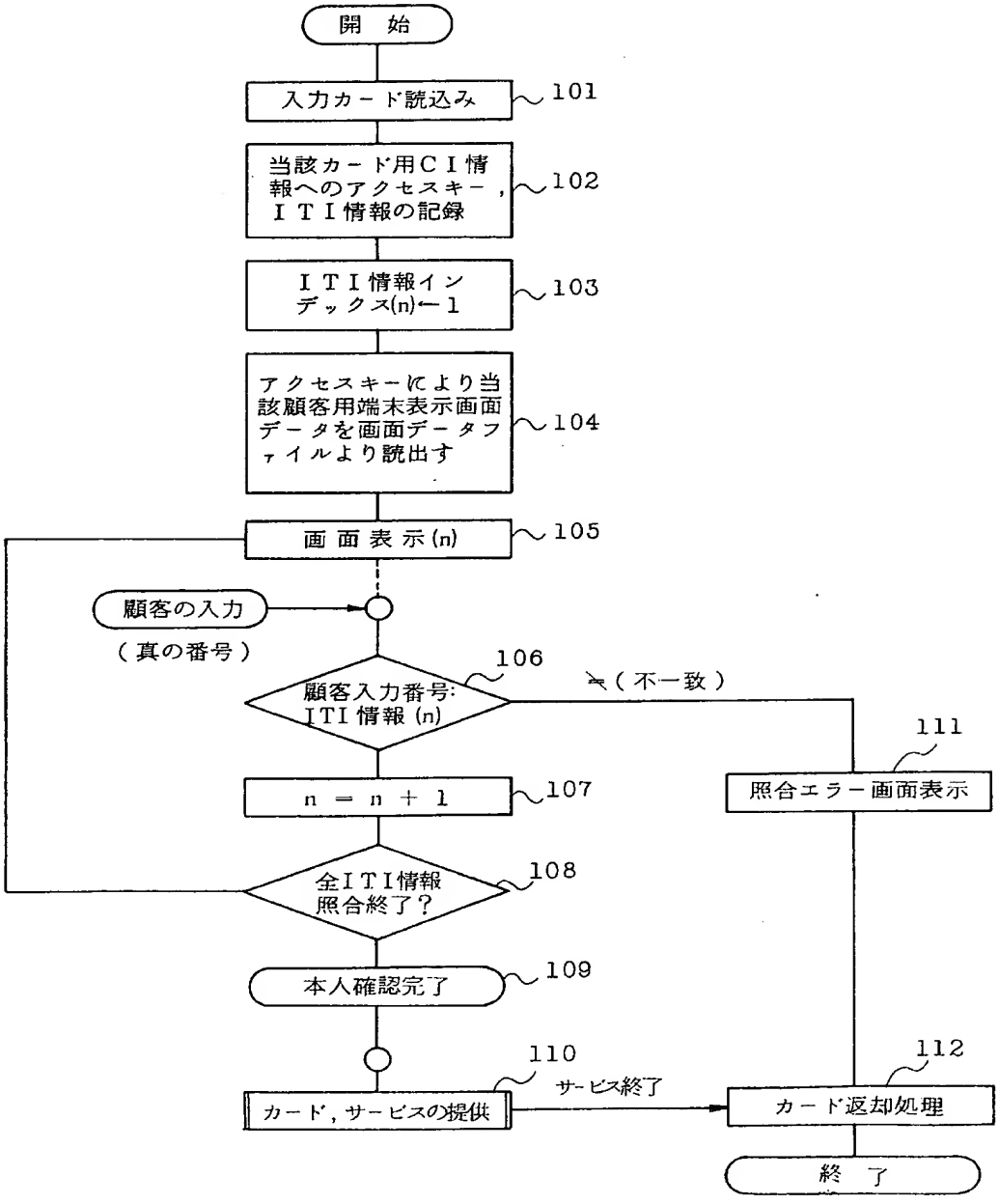
第１図は本発明の第１の実施例における自動取引システムの本人確認処理を示すフローチャート、第２図は本発明の第１の実施例における自動取引システムの構成図、第３図は本発明の第１の実施例における登録データ例図、第４図は本発明の第１の実施例におけるカード作成方法の説明図、第５図は本発明の第１の実施例における自動取引システムの機能構成図、第６図は本発明の第１の実施例における表示画面例図、第７図は本発明の第２の実施例における自動取引システムの機能構成図、第８図は本発明の第２の実施例におけるアクセスキーコードの構成例図、第９図は本発明の第２の実施例におけるアクセスコード情報例図、第１０図は本発明の第２の実施例における自動取引システムの本人確認処理を示すフローチャート、第１１図は本発明の第３の実施例における自動取引システムの機能構成図、第１２図は本発明の第

3の実施例におけるアクセスコード情報例図、第13図は本発明の第3の実施例における自動取引システムのアクセス時の処理を示すフローチャートである。

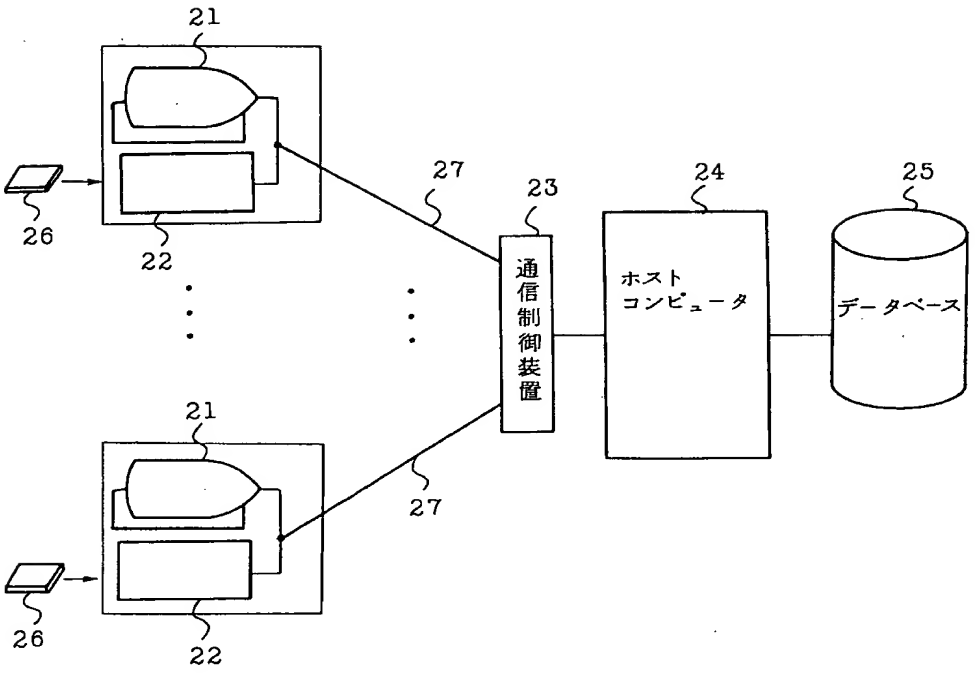
21：端末装置，22：カード読取装置，23：通信制御装置，24：ホストコンピュータ，25：データベース，26，41，51：カード，27：通信回線，52：カード読取部，53：出力画面データファイル，54：画面データ読込処理部，55：画面制御部，56：入力データ処理部，57：照合処理部，58：カード返却部，71：カード読取装置，72：カード読取部，73：アクセスコード情報（ACI）ファイル，74：ディスプレイ制御部，75：アクセスコード情報（ACI）読取部，76：乱数発生処理部，77：アクセスキーコード（AKG）作成処理部，78：入力コード照合処理部，79：キーボード読取部，80：サービス提供機能，81：端末装置のディスプレイ，82：端末装置のキーボード（KB）。

代理人　弁理士　磯村雅俊

第　1　図


開　始
入力カード読込み
101
当該カード用ＣＩ情報へのアクセスキー，ＩＴＩ情報の記録
102
ＩＴＩ情報インデックス(n)←1
103
アクセスキーにより当該顧客用端末表示画面データを画面データファイルより読出す
104
画面表示(n)
105
顧客の入力
（真の番号）
106
顧客入力番号:ITI情報(n)
≠（不一致）
111
照合エラー画面表示
n ＝ n ＋ 1
107
全ＩＴＩ情報照合終了？
108
本人確認完了
109
110
サービス終了
カード，サービスの提供
112
カード返却処理
終　了

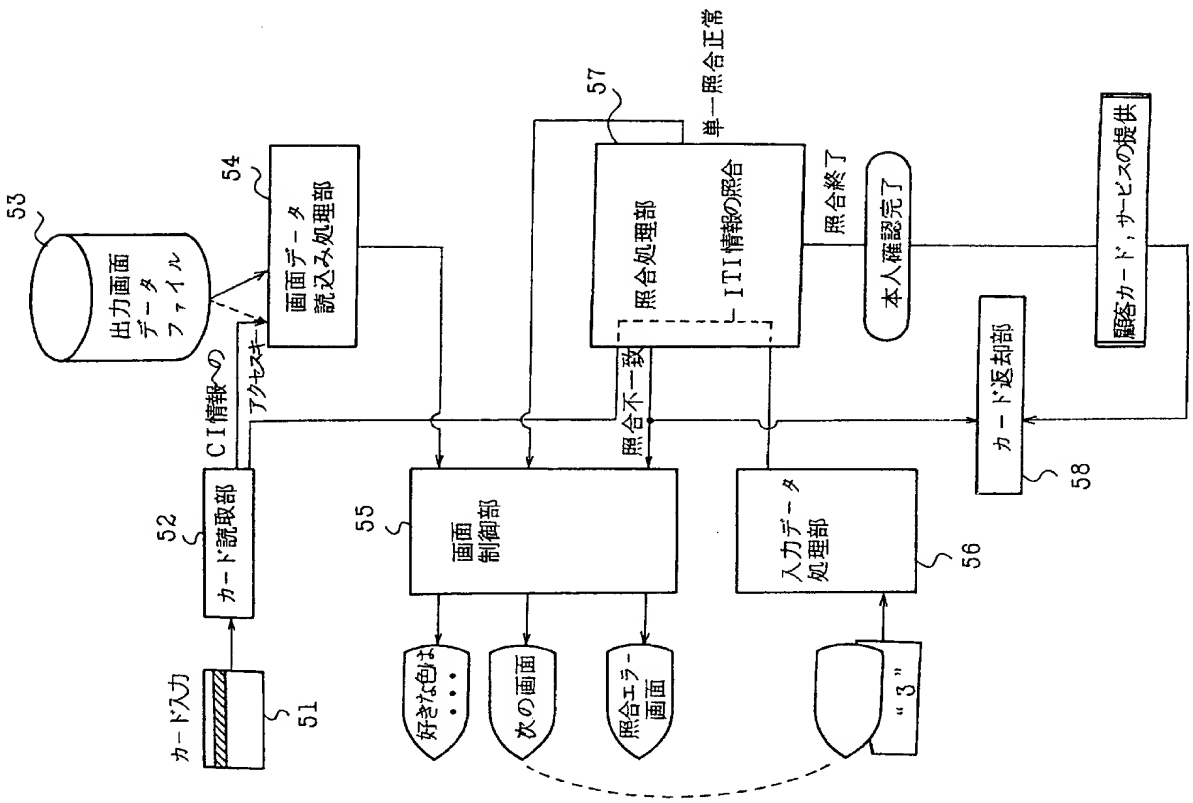
第　2　図



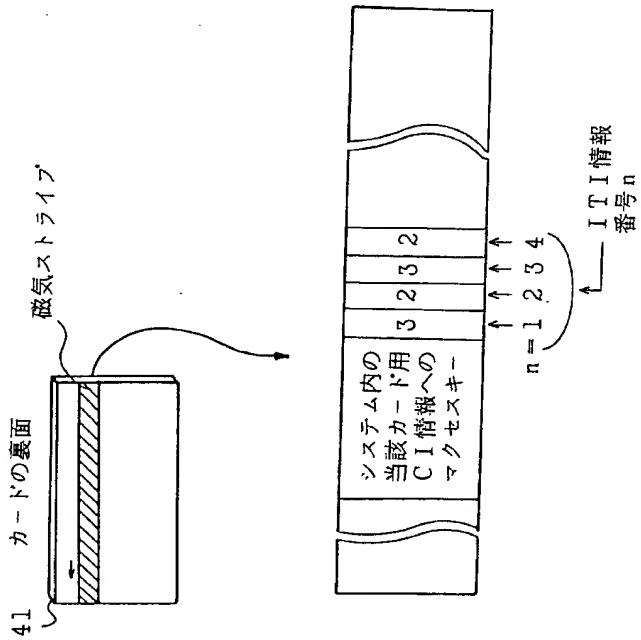
第　3　図

登録情報	ＩＴＩ	ＣＩ
暗証番号の１桁目	好きな色は黄色	赤，茶，白，黒・・
〃　２桁目	身長は１７５ｃｍ	180，160，165・・
〃　３桁目	家族は３人構成	4人，2人，1人・・
〃　４桁目	趣味はゴルフ	読書，車・・・

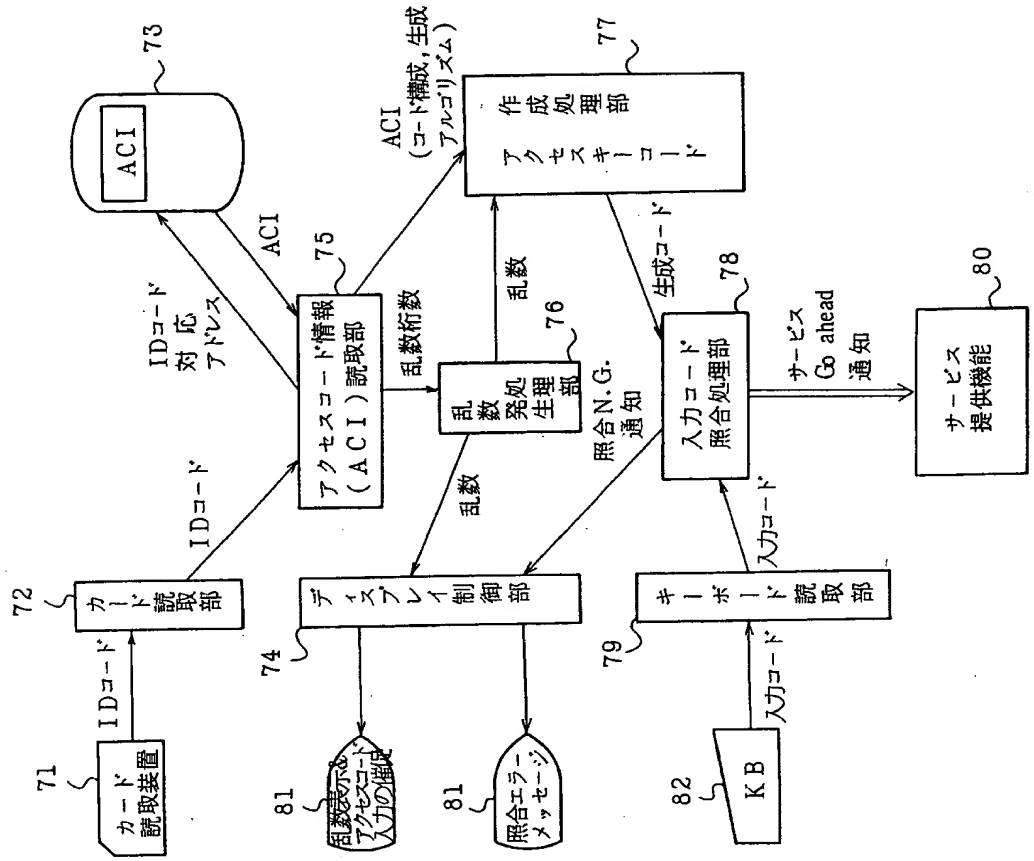
第 5 図


出力画面データファイル
53
画面データ読込み処理部
54
CI情報へのアクセスキー
カード読取部
52
カード入力
51
画面制御部
55
好きな色は・・・
次の画面
照合エラー画面
入力データ処理部
56
“3”
照合不一致
照合処理部
ITI情報の照合
57
単一照合正常
照合終了
本人確認完了
カード返却部
58
顧客カード，サービスの提供

第 4 図


磁気ストライプ
カードの裏面
41
システム内の当該カード用CI情報へのマクセスキー
3
2
3
2
n＝1 2 3 4
ITI情報番号n

第 7 図



第 6 図

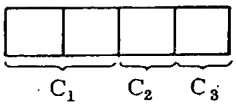
① 好きな色は何色ですか。
1＝赤
2＝茶
3＝黄
4＝白
5＝黒

② 身長は何cmですか。
1＝180cm
2＝175cm
3＝160cm
4＝165cm

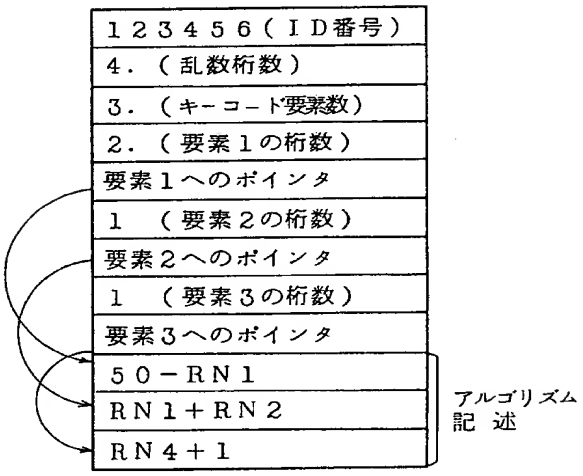
③ 家族は何人ですか。
1＝4人
2＝3人
3＝2人
4＝1人

④ 趣味は何ですか。
1＝読書
2＝ゴルフ
3＝車

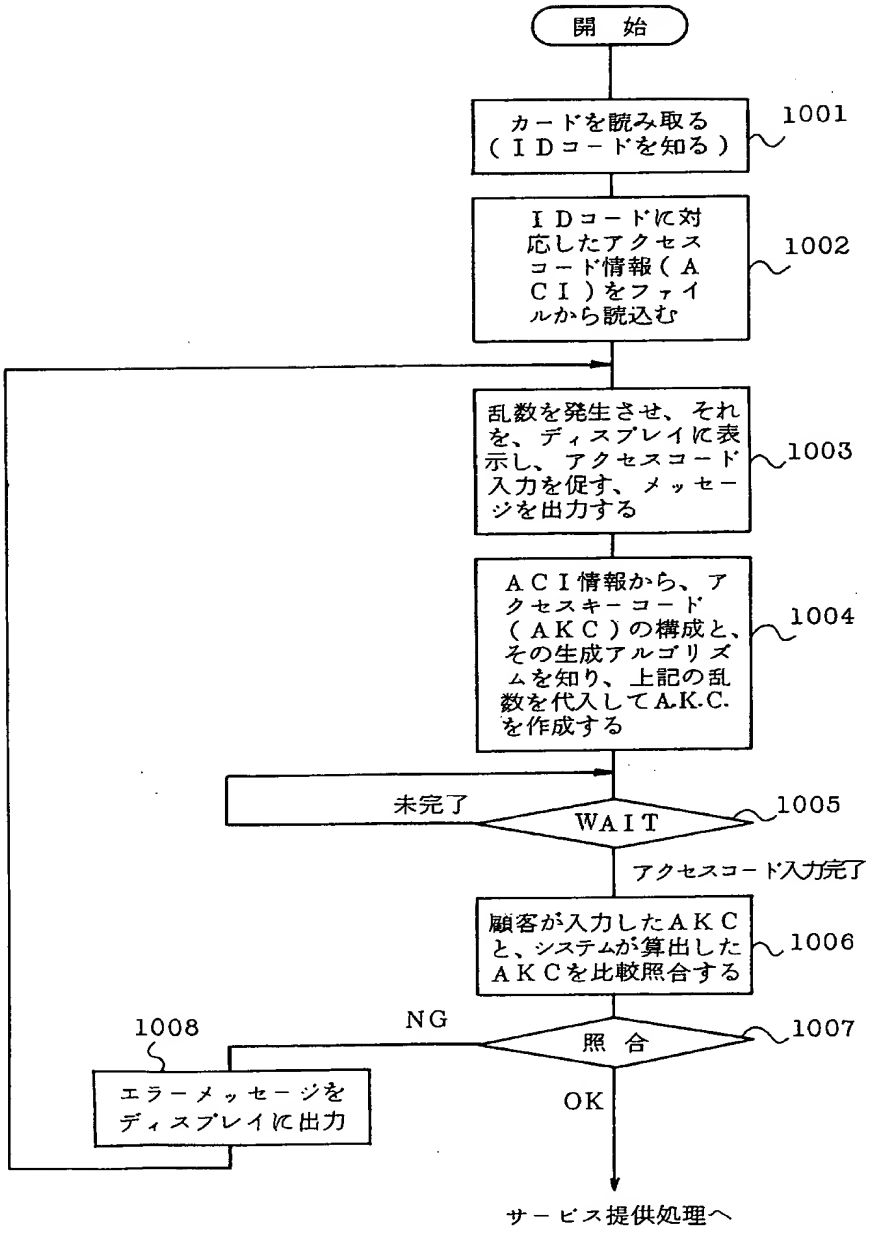
第　8　図


C1
C2
C3

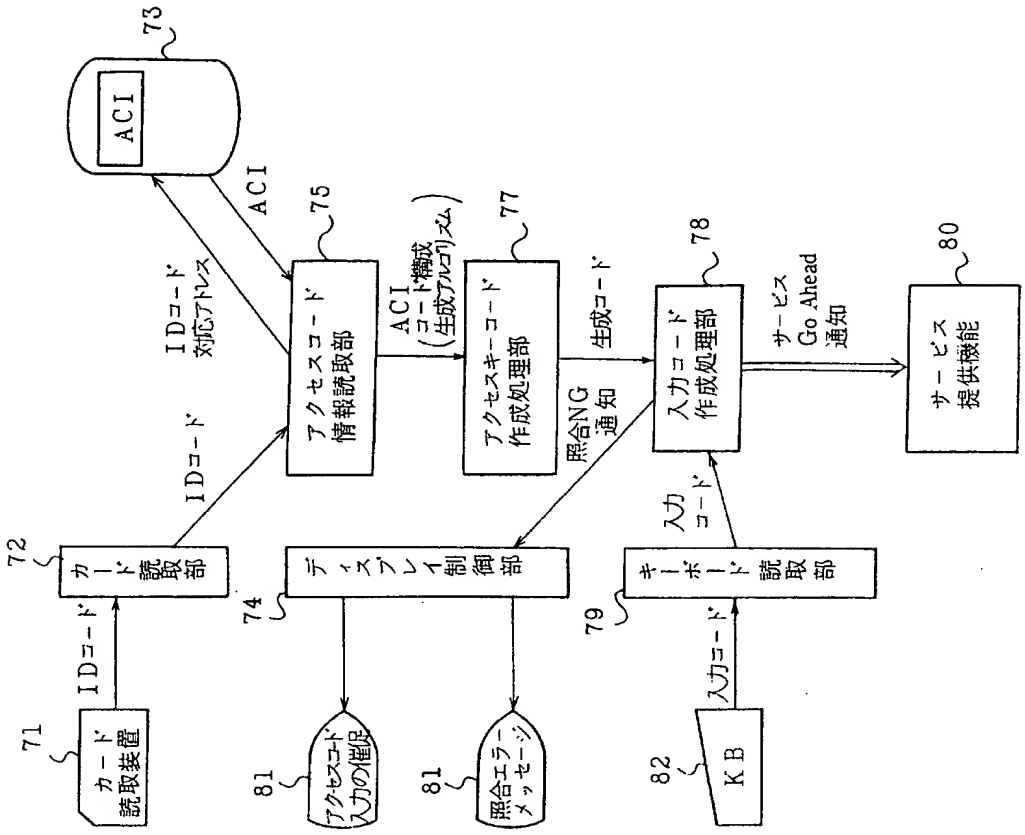
第　9　図


１２３４５６（ＩＤ番号）
４．（乱数桁数）
３．（キーコード要素数）
２．（要素１の桁数）
要素１へのポインタ
１　（要素２の桁数）
要素２へのポインタ
１　（要素３の桁数）
要素３へのポインタ
５０－ＲＮ１
ＲＮ１＋ＲＮ２
ＲＮ４＋１
アルゴリズム
記　述

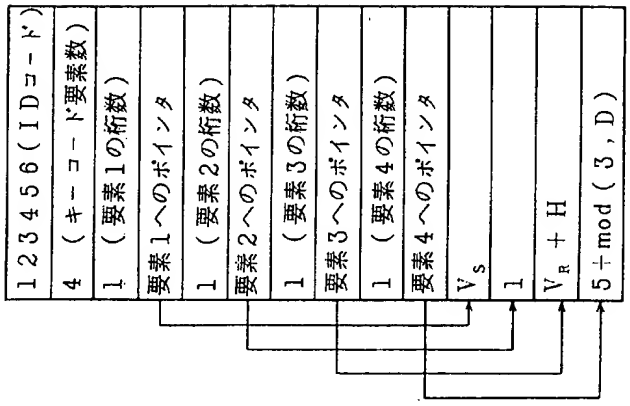
第　１０　図


開　始
カードを読み取る（ＩＤコードを知る）
1001
ＩＤコードに対応したアクセスコード情報（ＡＣＩ）をファイルから読込む
1002
乱数を発生させ、それを、ディスプレイに表示し、アクセスコード入力を促す、メッセージを出力する
1003
ＡＣＩ情報から、アクセスキーコード（ＡＫＣ）の構成と、その生成アルゴリズムを知り、上記の乱数を代入してA.K.C.を作成する
1004
未完了
WAIT
1005
アクセスコード入力完了
顧客が入力したＡＫＣと、システムが算出したＡＫＣを比較照合する
1006
NG
照　合
1007
1008
エラーメッセージをディスプレイに出力
OK
サービス提供処理へ

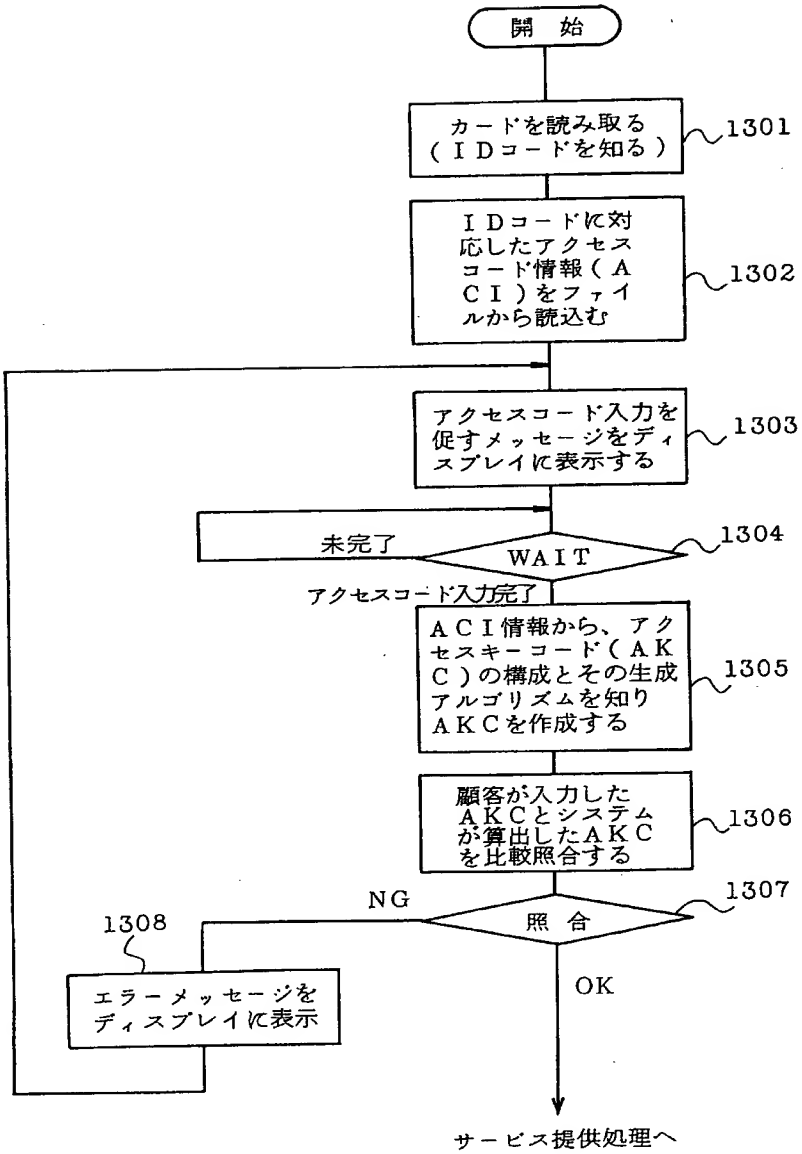
第 11 図


71
カード読取装置
IDコード
72
カード読取部
IDコード
IDコード
対応アドレス
73
ACI
ACI
74
ディスプレイ制御部
75
アクセスコード情報読取部
ACI
(コード構成
生成アルゴリズム)
77
アクセスキーコード作成処理部
生成コード
照合NG
通知
78
入力コード作成処理部
サービス
Go Ahead
通知
80
サービス提供機能
79
キーボード読取部
入力
コード
82
KB
入力コード
81
アクセスコード入力の催促
81
照合エラーメッセージ

第 12 図


1 2 3 4 5 6 (IDコード)
4 (キーコード要素数)
1 (要素1の桁数)
要素1へのポインタ
1 (要素2の桁数)
要素2へのポインタ
1 (要素3の桁数)
要素3へのポインタ
1 (要素4の桁数)
要素4へのポインタ
V_S
1
V_R + H
5 ÷ mod (3, D)

第　13　図


開　始
カードを読み取る（ＩＤコードを知る）
1301
ＩＤコードに対応したアクセスコード情報（ＡＣＩ）をファイルから読込む
1302
アクセスコード入力を促すメッセージをディスプレイに表示する
1303
未完了
WAIT
1304
アクセスコード入力完了
ＡＣＩ情報から、アクセスキーコード（ＡＫＣ）の構成とその生成アルゴリズムを知りＡＫＣを作成する
1305
顧客が入力したＡＫＣとシステムが算出したＡＫＣを比較照合する
1306
NG
照　合
1307
1308
エラーメッセージをディスプレイに表示
OK
サービス提供処理へ